UNITED STATES OF AMERICA v. WARRANT

2019 WL 4047615
United States District Court, N.D. California.
Case No.19-mj-71283-VKD-1
Filed 08/26/2019

ORDER RE APPLICATION FOR SEARCH WARRANT

VIRGINIA K. DEMARCHI United States Magistrate Judge

*1 The United States is investigating a suspected drug trafficking operation involving the illegal prescription and distribution of opioid pain relievers. The government submitted an application for a warrant under Federal Rule of Criminal Procedure 41 to search the residence of a suspected participant in the drug trafficking operation, and to seize and search certain electronic devices. The application included a request that the Court authorize law enforcement personnel to compel certain individuals to apply a biometric feature, such as a fingerprint, as necessary to unlock electronic devices within the scope of the warrant.

In support of its application, the United States submitted a brief filed in support of its pending petition for review by Judge James Donato of Magistrate Judge Kandis Westmore's denial of an application containing a similar request in *In the Matter of the Search of a Residence in Oakland, California*, No. 4:19-MJ-70053-KAW, Dkt. No. 2 (N.D. Cal. Jan. 23, 2019) ("U.S. Brief"). This Court invited the United States to submit additional briefing, if it wished, specific to this application, but the United States declined. Over the government's objection, this Court solicited the position of the Federal Public Defender regarding the Fourth and Fifth Amendment implications of compelling a suspect to use biometric features to unlock an electronic device.[1] The Federal Public Defender submitted its views in the form of a letter addressed to the Court ("FPD Letter"). The Court greatly appreciates the written submissions by both the United States and the Federal Public Defender on these issues.

After discussions with the Court concerning the original application, the United States submitted a revised application and warrant that limited the circumstances in which law enforcement personnel could compel the subject of the search to use his or her biometric features to unlock a device within the scope of the warrant, and on August 13, 2019, the Court signed the revised warrant. This order explains the Court's decision regarding the portion of the revised warrant directed to the compulsory application of biometric features to electronic devices within the scope of the warrant as it relates to the Fifth Amendment.

I. APPLICABILITY OF FIFTH AMENDMENT PRIVILEGE

The Fifth Amendment privilege against self-incrimination protects against the government's compulsion of incriminating testimony from an individual. *Fisher v. United States*, 425 U.S. 391, 408–09 (1976). For purposes of this application, the critical issue is whether compulsory application of a biometric feature is a testimonial communication. At present, there is no Supreme Court or Ninth Circuit authority specifically addressing the particular issue presented by this application.

A. Whether Use of Biometric Feature to Unlock Device Is Testimonial

*2 The United States argues that requiring an individual to place a finger on an electronic device or to face a device with his or her eyes open does not implicate Fifth Amendment concerns because fingerprints, facial features, or the details of an individual's iris or retina are merely physical

characteristics and thus should be considered physical evidence, not testimony. U.S. Brief at 8–9; *see also Doe v. United States*, 487 U.S. 207, 210 (1988) (observing that suspects may be compelled to provide a blood sample, a handwriting exemplar, and a voice exemplar, and to stand in a line up and to wear particular clothing, all of which are non-testimonial). The Federal Public Defender argues that compelling an individual to use his or her finger or face to unlock an electronic device is testimonial, because the compulsory act implies an assertion of fact—namely that the individual has control over the device and its contents. FPD Letter at 8–11.

So far as this Court is aware, only two federal appellate courts have addressed directly whether compelling an individual to decrypt an electronic device implicates the Fifth Amendment privilege, and they have disagreed on the answer. In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the Court of Appeals for the Eleventh Circuit concluded that "the decryption and production of the contents of ... hard drives is testimonial in character." 670 F.3d 1335, 1346 (11th Cir. 2012) ("Requiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the implied factual statements [regarding the defendant's role in placing contents on and encrypting the hard drive] noted above that could prove to be incriminatory"). However, in *United States v. Oloyede*, the Court of Appeals for the Fourth Circuit concluded that requiring a suspect to type in the password to her smartphone was not a testimonial communication. ---F.3d ---, 2019 WL 3432459, at *2–4 (4th Cir. 2019). ("Unlike a circumstance, for example, in which [suspect] gave the passcode to the agent for the agent to enter, here she simply used the unexpressed contents of her mind to type in the passcode herself.").

Several magistrate judges and district court judges across the country, as well as a few state courts, have recently addressed the specific question of whether compelled application of a biometric feature to an electronic device is a testimonial communication. This Court agrees with those courts that have concluded that requiring an individual to use a biometric feature to unlock an electronic device so that its contents may be accessed is an act of production that is inherently testimonial in the context of a criminal investigation. *See, e.g., In the Matter of the Search of a Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019); *In re Appl. for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017); *In the Matter of the Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, No. 1:19-mj-10441-REB, 2019 WL 2082709 (D. Idaho May 8, 2019), *vacated* --- F. Supp. 3d ---, 2019 WL 3401990 (D. Idaho July 26, 2019). Here, compelling an individual who is a target of the investigation to use his or her finger or face to unlock a device represents incriminating testimony within the meaning of the Fifth Amendment because it amounts to an assertion of fact that that the individual has the ability to unlock the device; which in turn makes it more like that the individual locked the device and put the material sought by the warrant on the device. *See, e.g., United States v. Spencer*, No. 17-cr-00259-CRB, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018) (explaining testimonial nature of compelling defendant to decrypt devices).

As the United States acknowledges, a consensus has emerged that a suspect may not be compelled to divulge his or her password to law enforcement, as that would require disclosure of the contents of the suspect's own mind. U.S. Brief at 12; *see also* FPD Letter at 9. The Court finds no meaningful distinction between unlocking a device with a password and unlocking a device with a biometric feature.[2] In each case, an individual must program the device to accept the input that unlocks it, whether that input is a password or the application of a finger, reflecting the same level of control over and connection to the device and its contents. The two means of locking and unlocking a device are functional equivalents.

*3 For these reasons, this Court disagrees with those courts that have concluded that compelling application of a biometric feature is no different than compelling the provision of non-testimonial physical evidence. *See, e.g., In the Matter of the Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, --- F. Supp. 3d ---, 2019 WL 3401990 (D. Idaho July 26, 2019); *In re Search Warrant Appl. for [Redacted Text]*, 279 F. Supp. 3d 800 (N.D. Ill. 2018); *In re Search of [Redacted] Washington, D.C.*,

317 F. Supp. 3d 523 (D.D.C. 2018). Unlike a fingerprint or blood sample, which is obtained for the purpose of identifying a particular individual, the only purpose of compulsory application of a biometric feature to a device is to obtain access to the device's contents; the government has no interest in obtaining the physical characteristic (e.g., the fingerprint) per se.

B. Whether the Foregone Conclusion Doctrine May Apply

In *Fisher*, the Supreme Court considered the government's efforts to compel production of an accountant's documents in the possession of a taxpayer's attorney. In that case, the government already knew of the existence of the documents and the taxpayer's access to them. In resolving the taxpayer's Fifth Amendment challenge to their production, the Supreme Court concluded that the privilege was not implicated because "the existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding [by production] that he in fact has the papers." *Fisher*, 425 U.S. at 411.

The "foregone conclusion" doctrine has developed in the context of cases involving the government's efforts to compel the production of documents by subpoena. *See id.* at 409–11; *United States v. Hubbell*, 530 U.S. 27, 34–38 (2000); *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004). As Judge Breyer of this District has observed recently, there is some confusion in the case law regarding what the relevant "foregone conclusion" is when the government does not seek the production of specific files, but instead seeks to compel access to an electronic device when the government has probable cause to believe that it contains evidence of a crime. *Spencer*, 2018 WL 1964588, at *3. The Federal Public Defender argues that the foregone conclusion doctrine cannot apply where the government does not know with "reasonable particularity" what the electronic device contains, even if a suspect's ability to unlock the device is known to the government, *unless* the government offers the suspect use and derivative use immunity. FPD Letter at 12–13. This Court agrees with Judge Breyer that the proper formulation of the "foregone conclusion" doctrine depends on the nature of the testimony that would be compelled by application of a biometric feature. For purposes of this application, the implied assertion of fact that renders use of a biometric feature testimonial is that the particular individual using his or her finger or face can unlock the device. The question then is whether that particular individual's ability to unlock a particular electronic device is a foregone conclusion. *See id.; see also State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016); *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3d Cir. 2017) (dicta).

Consideration of the "foregone conclusion" doctrine in the context of an application for a search warrant presents additional difficulties not ordinarily present when the Court considers an order compelling compliance with a document subpoena or, as in *Spencer*, an order compelling decryption of devices previously seized pursuant to a valid warrant. Specifically, the government may not know at the time of the application whether it will encounter circumstances at the time of execution demonstrating that a particular individual is capable of unlocking a particular device *before* law enforcement personnel seek to compel that individual to use his or her finger or face to unlock the device. This is the principal difficulty this application presents, and one that the Court has struggled to resolve in a manner that both respects the Fifth Amendment privilege and accommodates the government's legitimate interest in conducting a search that the Court has determined meets the requirements of the Fourth Amendment.

*4 The United States certainly runs the risk that the circumstances in which the devices are found will not support application of the "foregone conclusion" doctrine and that any compelled, incriminating testimony will be subject to suppression. The Court acknowledges that it would prefer the United States to apply for a court order compelling application of biometric features (or other means) to unlock an electronic device only after the device has been seized and after the record is more fully developed about the state of the government's knowledge. *See, e.g., In the Matter of the Search of a Residence in Aptos, California 95003*, No. 17-mj-70656-JSC-1, 2018 WL 1400401 (N.D. Cal. Mar. 20, 2018)

(deciding motion to compel decryption under the All Writs Act, 28 U.S.C. § 1651, following seizure of devices pursuant to search warrant), *aff'd sub. nom. United States v. Spencer*, No. 17-cv-00259-CRB, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018). But, this Court is not convinced that that approach is constitutionally *required* when the search warrant identifies the devices to be seized and the contents to be searched sufficiently to meet the requirements of the Fourth Amendment.

Judge Breyer suggests that the government should be required to show by clear and convincing evidence that a particular individual has the ability to decrypt or unlock a particular device. *Spencer*, 2018 WL 1964588, at *3. And he further observes that if the government is able to meet this standard, such that the act of decryption is a foregone conclusion and is not testimonial, then the government may not make direct use of the evidence that he or she has unlocked the device. *Id.* This Court does not reach either of these issues. Rather, the Court has authorized a search warrant that contains the direction it believes accurately describes the limited circumstances in which application of an individual's biometric feature can be compelled based on the facts presented in the government's application:

> During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are authorized to compel [named individuals] to apply their respective biometric feature(s) to a smartphone or other electronic device capable of being unlocked by such feature in order to search the contents of the device as authorized by this warrant, but only if the following conditions are met:
>
> > (1) the device is found on the person of one of the individuals named above or at the SUBJECT PREMISES; and
> >
> > (2) as to a particular device, law enforcement personnel have information that the particular individual who is compelled to apply his or her biometric feature(s) has the ability to unlock that device, such that his or her ability to unlock the device is a foregone conclusion.
>
> For purposes of this warrant, the application of a biometric feature refers to compelling an individual to depress his or her thumb-and/or fingerprints on the fingerprint reader of a device, or compelling an individual to face a device with his or her eyes open in order to activate the facial-, iris-, or retina-recognition feature of the device.

Warrant, Attach. B at 5.

IT IS SO ORDERED.

Dated: August 16, 2019

Footnotes

[1] The Court solicited the Federal Public Defender's views on the legal questions only, and not on the particular application, which is under seal.

[2] The Court disagrees with the United States that equating the function of typing in a passcode and pressing a finger to the fingerprint reader on an electronic device "contravenes Supreme Court case law." *See* U.S. Brief at 12. As the government concedes, the "case law" on which it relies is dicta that appears in a footnote responding to Justice Stevens's dissent in *Doe*. *Id.* at 13. This dicta refers to a distinction that the Supreme Court has not developed.